



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/315,901	05/20/1999	WOLFGANG DULTZ	2345/70	7089

26646 7590 01/12/2004

KENYON & KENYON
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER

REVAK, CHRISTOPHER A

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 01/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/315,901

Applicant(s)

DULTZ ET AL.

Examiner

Christopher A. Revak

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 29 September 2003.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ 6) ☐ Other: _____

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed as paper #9 on September 29, 2003 have been fully considered but they are not persuasive.

It is argued by the applicant that the teachings of Wright fail to disclose of "providing a secret random encryption binary encryption key provided by a key generator and recording the key on a first portable medium and a second portable medium as to define a first and second recorded key, a first user of the at least two users receiving the first portable medium with the first recorded key and a second user of the at least two users receiving the second portable medium with the second recorded key". The examiner respectfully disagrees for it is disclosed by Wright of a key generator which generates a shared private (secret random binary encryption) key for (storing on a medium) party A (first user's telecommunication device) and for (storing on a medium) party B (second user's telecommunication device)(as shown in Figure 3 and col. 5, lines 58-61). The keys are utilized (provided) for encrypting data packets (col. 4, lines 21-23). Once the keys are established, they are provided to cipher stream generators (first and second logistic device) which outputs a cipher stream which is used for bi-directional communications (as shown in Figure 1,3, col. 3, lines 17-31, and col. 5, line 67 through col. 6, line 2). The cipher stream generators (first and second logistic devices) are assigned to party A & B (first and second telecommunication devices) respectively as shown in Figures 1 and 3. The cipher stream generators (first

Art Unit: 2131

and second logistic devices) synchronizes the ordering so that the communications guarantee a correct order of delivery of the encrypted data sequence (col. 3, lines 32-38). The examiner additionally notes that Wright is not relied upon for teachings certain limitations of the claim, namely "recording a key on a portable medium" whereby the teachings of Samar are relied upon for this feature.

The applicant has additionally argued that there is not motivation to combine the teachings of Wright and Samar, the examiner respectfully disagrees. Samar is relied upon for disclosing the use of recording of a key on a portable medium. Samar further recites the benefits of recording the key in this manner for it is disclosed of by storing the private key on a smart card, it never leaves the device and can be safely maintained where it never passes through the computer system and consequently, in the event that the computer system is compromised, the key is not available to the intruder (col. 2, lines 20-28).

2. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., providing) are not recited in the rejected claim 13. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The applicant indicated that claim 13 contains analogous features to those of claim 1, however the examiner notes that claim 1 was amended to include the term "providing" instead of "generating" which currently recites "providing a secret binary encryption key"

Art Unit: 2131

whereby claim 13 was not amended in this manner and still currently recites "generating a random binary encryption key".

3. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). The applicant has argued that the teachings of Wright, Samar, Bennett, Menezes et al, and Schneier all fail to disclose "providing a secret random encryption binary encryption key provided by a key generator and recording the key on a first portable medium and a second portable medium as to define a first and second recorded key, a first user of the at least two users receiving the first portable medium with the first recorded key and a second user of the at least two users receiving the second portable medium with the second recorded key" in regards to the combination of the teachings of Wright, Samar, Bennett, Menezes et al, and Schneier at applied to claims 1-20. The applicant has attacked the cited references individually and the examiner is relying upon the combination of the teachings to meet the applicant's claim limitations and has provided the necessary motivation for reasons to combine the teachings as is taught in the references. Please refer to the rejections below for citations and motivational benefits.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-3,7-11,13,14,18, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wright in view of Samar.

As per claim 1, it is disclosed by Wright of a key generator which generates a shared private (secret random binary encryption) key for (storing on a medium) party A (first user's telecommunication device) and for (storing on a medium) party B (second user's telecommunication device)(as shown in Figure 3 and col. 5, lines 58-61). The keys are utilized (provided) for encrypting data packets (col. 4, lines 21-23). Once the keys are established, they are provided to cipher stream generators (first and second logistic device) which outputs a cipher stream which is used for bi-directional communications (as shown in Figure 1,3, col. 3, lines 17-31, and col. 5, line 67 through col. 6, line 2). The cipher stream generators (first and second logistic devices) are assigned to party A & B (first and second telecommunication devices) respectively as shown in Figures 1 and 3. The cipher stream generators (first and second logistic devices) synchronizes the ordering so that the communications guarantee a correct order of delivery of the encrypted data sequence (col. 3, lines 32-38). The examiner asserts that the cipher stream generators (first and second logistic devices) check the private (first and second) keys that they have been applied (inserted) correctly because Wright discloses that the communication channel must be able to guarantee a correctly ordered delivery of encrypted data packets and if synchronization is lost, the encrypted

Art Unit: 2131

data packets may be lost (col. 3, lines 35-40). The teachings of Wright are silent in disclosing of recording a key on a portable medium. This feature is disclosed by Samar of recording a private key on a smart card which is used to encrypt communications (col. 3, lines 22-31, 34-38). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to store private keys on an external device such as a smart card in order to protect the integrity of the key. Samar recites motivation for use of this concept by disclosing that by storing the private key on a smart card, it never leaves the device and can be safely maintained where it never passes through the computer system. In the event that the computer system is compromised, the key is not available to the intruder (col. 2, lines 20-28). It is obvious that the teachings of Wright would have benefitted from the teachings of Samar as a means to protect the integrity of the private key from being compromised by an unauthorized user.

As per claims 2 and 14, it is disclosed by Wright that the public (first and second) keys must be synchronized so that the cipher stream generators (first and second logistic devices) can properly encrypt (and decrypt) the transmitted data (col. 3, lines 31-38).

As per claims 3 and 19, it is disclosed by Wright of generating (by a key generator) secondary private (additional secret random binary encryption) keys which are used to encrypt information for transmission over a communications channel (col. 4, lines 10-16). The secondary private (additional) keys are generated and it is checked to see if they are properly synchronized between the two parties so that the correct key is used for decryption (col. 6, lines 2-18). The teachings of Wright are silent in disclosing of recording a key on a portable medium. This feature is disclosed by Samar of recording a private key on a smart card (by inserting it into the computer) which is used

Art Unit: 2131

to encrypt communications (col. 3, lines 22-31, 34-38). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to store private keys on an external device such as a smart card in order to protect the integrity of the key. Samar recites motivation for use of this concept by disclosing that by storing the private key on a smart card, it never leaves the device and can be safely maintained where it never passes through the computer system. In the event that the computer system is compromised, the key is not available to the intruder (col. 2, lines 20-28). It is obvious that the teachings of Wright would have benefitted from the teachings of Samar as a means to protect the integrity of the private key from being compromised by an unauthorized user.

As per claim 7, the teachings of Wright disclose of two parties being involved in an encrypted system utilizing a stream cipher. The teachings of Samar are relied upon for the use of storing the private key on a smart card (portable media)(col. 3, lines 22-31, 34-38).

As per claim 8, the teachings of Samar are relied upon for the use of storing the private key on a smart card (semiconductor storage device)(col. 3, lines 22-31, 34-38).

As per claims 9 and 18, the teachings of Wright are relied upon for the use of a key generator which generates a shared private (secret random binary encryption) key for (storing on a medium) party A (first user's telecommunication device) and for (storing on a medium) party B (second user's telecommunication device)(as shown in Figure 3 and col. 5, lines 58-61). The examiner asserts that a keyboard is used in the teachings of Wright since there is an interface for a user to communicate with a computer whereby the user can use the keyboard to enter commands into the computer to dictate how the key generator will work. The teachings of Samar are relied upon for the use of storing

the private key on a smart card (portable media)(col. 3, lines 22-31, 34-38). It is shown in Figure 1 of Samar of the use of atleast 3 (number of selectable) smart cards.

As per claim 10, the teachings of Wright disclose of a key generator which generates a shared private (secret random binary encryption) key for (storing on a medium) party A (first user's telecommunication device) and for (storing on a medium) party B (second user's telecommunication device)(as shown in Figure 3 and col. 5, lines 58-61). The teachings of Wright are silent in disclosing that the key generator is accessible to the public. The examiner hereby takes official notice that the knowledge of a key generator is readily available to the public. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to make public knowledge of a key generation process. It is notoriously well known that the particular algorithm is public knowledge for a key generation process, what is unknown is the information which is submitted into the key generator which produces the random value which is used to encrypt the stream of data. Based on infinite possibilities for a generated key value makes it hard for a hacker to crack the generator in order to obtain the key. It is obvious that the teaching of Wright make known to the public the key generator, but conceal the information regarding to the value of the information inserted into the key generator in order to maintain security of the encrypted transmission of data.

As per claim 11, the teachings of Samar are relied upon for the use of storing the private key on a smart card (magnetic strip card)(col. 3, lines 22-31, 34-38). The examiner asserts that upon entry of the smart card (portable media), the key is used to encrypt information. The teachings of Wright are relied upon for the use of a key generator which generates a shared private (secret random binary encryption) key for (storing on a medium) party A (first user's telecommunication device) and for (storing on

Art Unit: 2131

a medium) party B (second user's telecommunication device)(as shown in Figure 3 and col. 5, lines 58-61).

As per claim 13, it is disclosed by Wright of a key generator which generates a shared private (secret random binary encryption) key for (storing on a medium) party A (first user's telecommunication device) and for (storing on a medium) party B (second user's telecommunication device)(as shown in Figure 3 and col. 5, lines 58-61). Once the keys are established, they are provided to cipher stream generators (first and second logistic device) which outputs a cipher stream which is used for bi-directional communications (as shown in Figure 1,3, col. 3, lines 17-31, and col. 5, line 67 through col. 6, line 2). The cipher stream generators (first and second logistic devices) are assigned to party A & B (first and second telecommunication devices) respectively as shown in Figures 1 and 3. The cipher stream generators (first and second logistic devices) synchronizes the ordering so that the communications guarantee a correct order of delivery of the encrypted data sequence (col. 3, lines 32-38). The examiner asserts that the cipher stream generators (first and second logistic devices) check the private (first and second) keys that they have been applied (inserted) correctly because Wright discloses that the communication channel must be able to guarantee a correctly ordered delivery of encrypted data packets and if synchronization is lost, the encrypted data packets may be lost (col. 3, lines 35-40). The teachings of Wright are silent in disclosing of recording a key on a portable medium. This feature is disclosed by Samar of recording a private key on a smart card which is used to encrypt communications (col. 3, lines 22-31, 34-38). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to store private keys on an external device such as a smart card in order to protect the integrity of the key. Samar recites motivation for use of this concept by disclosing that by storing the private key on

a smart card, it never leaves the device and can be safely maintained where it never passes through the computer system. In the event that the computer system is compromised, the key is not available to the intruder (col. 2, lines 20-28). It is obvious that the teachings of Wright would have benefitted from the teachings of Samar as a means to protect the integrity of the private key from being compromised by an unauthorized user.

3. Claims 4,5,15, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wright in view of Samar in further view of Bennett as supported by Menezes et al.

The teachings of Wright disclose of a key generator, but fail to disclose that the key generator uses a beam generator or emissions of photons. The teachings of Bennett disclose of beamsplitters which produce photon pulses (emissions)(col. 2, lines 55-58,65-67). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a specific key generator which is used to generate keys. Menezes et al recites motivation for the use of key generator by reciting a true random bit generator requires a naturally occurring source of randomness which makes it difficult to exploit the randomness of a hardware or software device (pg 171). Using pseudorandom bit generators are sufficient means, but have proven not to be cryptographically secure (pg 173). It is obvious for the teachings of Wright to have utilized a random key generator such as based on a beam splitter or photon emissions as taught by Bennett and based on the reasons recited by Menezes et al that makes it difficult to exploit the key generation process.

Art Unit: 2131

4. Claims 6 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wright in view of Samar in further view of Menezes et al.

The teachings of Wright disclose of a key generator, but fail to disclose that the key generator uses radioactive decay. The teachings of Menezes et al disclose of a key generator which is based on an elapsed time between emission of particles during radioactive decay (pg 172). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a specific key generator which is used to generate keys. Menezes et al recites motivation for the use of this particular type of key generator by reciting a true random bit generator requires a naturally occurring source of randomness which makes it difficult to exploit the randomness of a hardware or software device (pg 171). Using pseudorandom bit generators are sufficient means, but have proven not to be cryptographically secure (pg 173). It is obvious for the teachings of Wright to have utilized a random key generator such as based on radioactive decay for reasons recited by Menezes et al that makes it difficult to exploit the key generation process.

5. Claims 12 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wright in view of Samar in further view of Schneier.

The teachings of Wright disclose of a key generator which generates a shared private (secret random binary encryption) key for (storing on a medium) party A (first user's telecommunication device) and for (storing on a medium) party B (second user's telecommunication device)(as shown in Figure 3 and col. 5, lines 58-61). The teachings are silent in disclosing that the key is used only once. In a related teaching, Schneier discloses of using a one-time pad (key) in a stream cipher (pg 197). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been

motivated to apply a key which is used only once in order to increase security of the encrypted data transmission. The teachings of Schneier recited motivation for use of the one-time pad (key) by disclosing that if the keystream generator produces a stream of random bit, it produces a one-time pad (key) which provides perfect security and the closer the keystream generator's output is randomly produced, it is harder for a hacker to crack it (pg 197). It is obvious that the teachings of Wright would have produced a key which is only used once for reasons of providing a strong encryption scheme which would be near impossible to break as is taught by Schneier.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

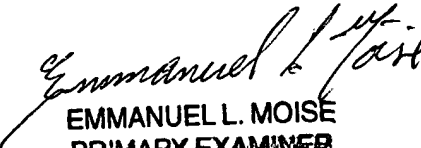
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 703-

Art Unit: 2131

305-1843. The examiner can normally be reached on M-Th, 6:30a-4:00p, alt. Fr,
6:30am-3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9586. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.


EMMANUEL L. MOISE
PRIMARY EXAMINER

CR



January 4, 2004